I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Copyright, Data Protection, and Privacy with Digital Rights Management and Trusted Systems: Negotiating a Compromise between Proprietors and Users

SAIF M. KHAN*

Abstract: Digital rights management ("DRM") and trusted systems offer the promise of enhanced protection of virtually any form of data, but at the same time jeopardize user rights to this data and user privacy. Finding the right medium that appropriately balances these concerns has proven difficult. This note first explores the role of the current legal framework regulating DRM technologies and trusted systems. The note then discusses how DRM can protect copyright owners' rights. These measures and their associated legal enforcement are part of a battle between proprietary appliance-like systems that are a product of the DRM lockdown, and the commons-based model that dominates the Internet and information networks today. The note next explores how trusted systems can protect personal information, much like how DRM has been used to safeguard creative content. The note then elaborates on how DRM and trusted systems may harm the privacy interests of users performing transactions with these systems. The note ultimately concludes with a discussion on technological implementations and legal reforms that could accommodate both data owners and users.

---

* Saif Khan is a J.D. candidate at The Ohio State University Moritz College of Law. He earned both a B.A. and M.A. in Physics from Wayne State University. The author thanks Peter Swire, Martha Landesberg and Dennis Hirsch for their helpful comments and suggestions.

I. INTRODUCTION

This note explores the ability of digital rights management ("DRM") technologies, and particularly, trusted systems, to protect content or sensitive data while also potentially intruding on the privacy of users who access such information or databases containing this information.

DRM encompasses technological measures built into physical devices that restrict content usage, such as access controls, copy restrictions, embedded identifications in content, and surveillance.[1] More specific examples of these technologies include digital watermarks, encryption, and restrictions to content access based on time, location, method of access, or content amount. In particular, trusted systems are focused applications of DRM technologies which require devices to obey rules defined by owners.[2]

Corporations often have incentives to use DRM in order to obtain extra royalties through enhanced protection of content. Some believe this use to be a natural extension of copyright, while others believe that copyright was never intended to reach so far. In addition to protecting creative content, corporations may similarly implement trusted systems to safeguard personal information. On the other hand, corporations also like to use data for marketing, and therefore may not want trusted systems because they are expensive to build and maintain. Finally, many privacy advocates are concerned that DRM systems and trusted systems can be inimical to the privacy interests of users who attempt to access these systems, depending on system design.

Part II surveys the current legal framework for regulating and enforcing DRM. The DRM anti-circumvention provisions of the Digital Millennium Copyright Act constitute the primary legal enforcement of DRM.

In Part III, the note explores how DRM technologies can greatly expand the protection of content. Part III also explains, however, that such a DRM lockdown raises a number of policy concerns including

---

[1] Graham Greenleaf, *IP, Phone Home: The Uneasy Relationship Between Copyright and Privacy, Illustrated in the Laws of Hong Kong and Australia*, 32 HONG KONG L.J. 35, 43-46 (2002).

[2] TARLETON GILLESPIE, WIRED SHUT: COPYRIGHT AND THE SHAPE OF DIGITAL CULTURE 52 (2007).

the normatively proper scope of a copyright owner's rights and DRM's ultimate effect on creativity.[3]

Just as DRM systems can protect creative content, Part IV examines how trusted systems can also safeguard sensitive personal information. Specifically, trusted systems can provide enhanced protection of virtually any type of information – including digital content and personal information such as medical and financial records – by implementing a layered system of access controls.[4] This enhanced privacy regime makes it much harder for internal employees or external hackers to retrieve sensitive personal information from company databases.

Although DRM and trusted systems can provide many protective benefits for content and data owners, Part V of the note discusses how certain types of DRM and trusted systems may create privacy risks to users who access protected content or data by exposing users' personal information during authentication. The ultimate balance between content owners' rights and users' rights, however, is sensitive to the type of trusted system implemented.[5] In some versions, proprietors can conduct surveillance of all users engaging in data transactions or accessing their networks or databases simply by configuring DRM to collect these users' ID data.[6] Other variants prevent owners from receiving these reports.[7] A principal risk is the surveillance of *all* infringing and/or illegal user activities with respect to content and data.[8] This surveillance could shrink the private sphere of personal activities and transactions that the law was unable to regulate prior to the existence of DRM.[9]

In Part VI, the note closes with a commentary on finding the right medium in the private sphere that best accommodates content owners' rights and users' privacy interests. Specifically, this Part

---

[3] In this note, the "DRM lockdown" refers to the ubiquitous application of DRM technologies.

[4] GILLESPIE, *supra* note 2, at 53.

[5] Kim Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J.L. & TECH. 123, 169 (2004).

[6] Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J., 575, 585-86 (2003).

[7] *Id.*

[8] Greenleaf, *supra* note 1, at 67.

[9] *Id.*

explores DRM designs and legal reforms that could help achieve this balance.

II. EXISTING LEGAL ENFORCEMENT OF DRM TECHNOLOGIES

The information infrastructure, which refers to communication networks, devices and software that govern the transfer of information, was initially unregulated and content passed through the infrastructure unencumbered. For example, internet protocols, which form one part of the information infrastructure, for most of their history were not proprietary and were developed through publicly-funded research.[10] Justifying a need to render the information infrastructure conducive to the delivery of digital content without copying, lobbyists proposed the development of a regulatory framework that would enforce technological protections of content flow within the information infrastructure.[11]

The WIPO Copyright Treaty of 1996 ("WCT") requires member countries to implement laws banning DRM circumvention.[12] As a World Intellectual Property Organization ("WIPO") member, the United States Congress passed the Digital Millennium Copyright Act of 1998 ("DMCA").[13] The DMCA prohibits circumvention of technological measures that control access to a work[14] and its related preparatory activities, such as manufacturing, importing, offering to the public, providing, or otherwise trafficking in technologies that circumvent access control measures.[15] Such prohibitions are generally imposed regardless of whether the circumvention or preparatory activities result in or are intended for copyright infringement.[16] Additionally, the DMCA prohibits preparatory activities for

---

[10] YOCHAI BENCKLER, THE WEALTH OF NETWORKS 412 (2006).

[11] *Id.* at 395, 413.

[12] World Intellectual Property Organization Copyright Treaty art. 11, Dec. 20, 1996.

[13] *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 5, 17, 28, and 35 U.S.C.).

[14] 17 U.S.C. § 1201(a)(1) (2000).

[15] 17 U.S.C. § 1201(b)(1) (2000).

[16] Steve P. Calandrillo & Ewa M. Davison, *The Dangers of the Digital Millennium Copyright Act: Much Ado about Nothing?*, 50 WM. & MARY L. REV. 349, 364 (2008).

circumventing copy control measures that allow access to copyrighted works but restrict copying.[17]

The DMCA has generated much controversy, yet it has thus far survived constitutional challenges. Although the Supreme Court has yet to rule on the issue, the U.S. Court of Appeals for the Second Circuit, arguably the most influential federal circuit court on copyright,[18] affirmed the district court ruling in *Universal City Studios v. Corley*. There, the Second Circuit held that an injunction against distributing software designed to circumvent DVD security technology did not violate the plaintiff's claimed fair use rights,[19] and that the injunction's burden on speech did not outweigh government interests and therefore did not violate the First Amendment.[20] However, *Corley* was not an ideal factual scenario in which to challenge the DMCA because it dealt with distribution as opposed to a technology directly geared at restricting fair uses.[21] Thus, the DMCA remains susceptible to challenge in future lawsuits.

Other nations and supra-national entities have enacted similar provisions. The E.U. passed three directives[22] that include anti-

---

[17] 17 U.S.C. § 1201(b)(1) (2000).

[18] Georgia K. Harper, The Copyright Crash Course, *Building On Others' Creative Expression: Professional Fair Use after Texaco* n. 11, http://copyright.lib.utexas.edu/tex2.html (last visited April 8, 2010).

[19] Universal City Studios Inc. v. Corley, 273 F.3d 429, 458-59 (2d Cir. 2001). The doctrine of fair use allows consumers a limited use of copyrighted works without permission from copyright owners. For example, consumers can incorporate part of a copyrighted work in a subsequent new work. A four-factor test governs whether a particular use of a copyrighted work is a fair use. 17 U.S.C. § 107 (2000).

[20] *Corley*, 273 F.3d at 458.

[21] *Id.* at 459-60.

[22] *See* Council Directive 91/250/EEC of May 14, 1991, on the Legal Protection of Computer Programs,1991 O.J.E.U. (L 122) 42, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:EN:HTML; Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001, on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society,2001 O.J.E.U. (L 167) 10, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF; Directive 98/84/EC of the European Parliament and of the Council of November 20, 1998, on the Legal Protection of Services Based on, or Consisting of, Conditional Access, 1998 O.J.E.U.. (L 320) 54, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0084:EN:HTML. These directives were not self-executing and required E.U. member states to enact legislation to achieve the directives' aims.

circumvention provisions, including provisions prohibiting actual circumvention of effective measures as well as preparatory activities associated therewith, such as circulation, production, promotion, and possession for commercial purposes.[23] Japan's implementation of the WCT is less sweeping than the U.S. or the E.U. In contrast to the U.S. approach, Japan neither prohibits circumvention of access control nor prohibits circumvention of uses falling under copyright exemptions such as fair uses.[24]

III. PERSPECTIVES ON COPYRIGHT AND THE DRM LOCKDOWN

Proponents of DRM and the so-called proprietary model cite several rationales supporting the implementation of the DRM lockdown in view of copyright owner rights. Principally, DRM can potentially solve the problem of the non-exclusivity of digital content. An expanded role of DRM also complements a generally expanded role for intellectual property rights in protecting business interests. On the other hand, opponents of the DRM lockdown advocate openness and suggest that the costs outweigh these perceived benefits. These costs include encroachment on the fair use doctrine and a transformation from a commons-based model to a proprietary model favoring big business at the expense of the public.

A. HOW DRM CAN PROTECT CONTENT OWNERS' RIGHTS

Normally, digital content is a non-exclusive good—one which current technology allows for the creation of an unlimited number of perfect copies at a negligible cost to a copier. Such non-exclusivity results in consumers committing wide-scale acts of copyright infringement. Additionally, non-exclusivity limits the ways that content owners can market digital content.

Since DRM has the ability to restrict users' ability to access and/or copy content, DRM can render such content exclusive. In this scenario, infringement is curtailed because it becomes more technically difficult and expensive – even illegal – under the DMCA. Moreover, DRM's ability to transform digital content into an exclusive

---

[23] Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 AM. J. COMP. L. 323, 335-36 (2004).

[24] Yuko Noguchi, *Freedom Override by Digital Rights Management Technologies: Causes in Market Mechanisms and Possible Legal Options to Keep a Better Balance*, 11 INTELL. PROP. L. BULL. 1, 9-10 (2006).

good can enhance the content's marketability, enabling content owners to generate varied business models.[25] For example, content owners could utilize price-discrimination models, which could increase social welfare by providing wider access to content.[26] Additionally, content exclusivity may reduce transaction costs associated with content distribution. For example, such exclusivity could reduce the costs of rights clearance by providing direct licensing online, as opposed to utilizing intermediaries for distributing copyrighted works.[27]

In the past decade-and-a-half, proponents of this proprietary model have vigorously lobbied Congress to expand the scope of intellectual property rights[28] and technological regulation. These lobbyists, primarily from the film and music industries, cite the need to protect their business models and argue that enhanced legal protection is a legitimate method to fortify the incentive-based model.[29]

Trusted systems are one implementation of the proprietary model; these systems turn "personal computers away from being purely general-purpose computation devices toward being devices with factory-defined behaviors vis-à-vis predicted-use patterns, like glorified televisions and CD players."[30] Some copyright holders value this transformation since computers become tools for the dissemination of content on the copyright holders' terms. These terms can include implementing factory-defined behaviors that prevent copying.

Lobbyists supporting the proprietary model also hope for a stronger regulatory framework that favors the development of such specialized devices. In 2002, the U.S. Senate considered the Broadband and Digital Television Promotion Act ("CBDTPA"), which would have required computer manufacturers to include trusted

---

[25] *Id.* at 5-6.

[26] *Id.*

[27] *Id.*

[28] One caveat to note is that although patent protection underwent an expansionary trend during the 1990s and early 2000s, this trend has reserved in recent years. Copyrights, on the other hand, continue to receive term extensions and other expansions in scope.

[29] BENCKLER, *supra* note 10, at 380-81.

[30] *Id.* at 397.

systems in their computers that would render certain types of software incompatible with the computer chip.[31] However, that bill never came out of the Senate Judiciary Committee. Another pro-DRM effort was more successful, at least initially: Hollywood's intense lobbying convinced the Federal Communications Commission (FCC) to require all devices capable of receiving digital television signals from a television to conform to a particular trusted system standard.[32] This would have been accomplished in part by including broadcast flags in the digital signals that indicate any restrictions on content stored therein, particularly whether the signals can be recorded. The U.S. Court of Appeals for the D.C. Circuit struck down the regulations, however, on grounds that the FCC had exceeded its authority, which extends only to the regulation of transmissions and not the devices that receive them.[33]

Finally, content owners utilize contracts to strengthen their property rights.[34] For example, copyright owners utilize click-wrap (shrink wrap) licenses to impose conditions on content, artifacts, and devices, although many of these contracts have questionable enforceability due to the inequities and power differentials involved.[35] Certain DRM developers and copyright owners may work in tandem and utilize licenses to ensure that such distribution of content is allowed only with a particular form of DRM.[36] Content owners may also enter into distribution licenses with intermediaries requiring them to maintain DRM protections.[37]

---

[31] Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. 1st Sess. § 5 (2001). Lobbyists had earlier proposed the Security Systems Standards and Certification Act; however, Congress never considered that version of the bill.

[32] 47 C.F.R. § 73.9002(b) (2008).

[33] Am. Library Ass'n v. Fed. Comm'ns Comm'n, 406 F.3d 689 (D.C. Cir. 2005).

[34] Greenleaf, *supra* note 1, at 42.

[35] *Id.* Although few courts have ruled on the validity of click-wrap licenses, most have upheld them. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996) (upholding the validity of a click-wrap license); *contra* Bragg v. Linden Research, Inc., 487 F.Supp.2d 593, 611 (E.D. Pa. 2007) (finding aspects of a click-wrap contract unconscionable and therefore unenforceable).

[36] Greenleaf, *supra* note 1, at 42 (citing Bechtold, *supra* note 23, at part 4).

[37] *Id.* at 42.

B. OPPOSITION TO THE DRM LOCKDOWN

Lawrence Lessig has noted that the future of innovation is in jeopardy because of overregulation by a combination of both copyright and DRM.[38] DRM can countermand copyright exemptions and otherwise non-infringing uses, as well as free access to copyrighted materials.[39] According to Lessig, the zone of unregulated content, such as reading a public-domain work in the pre-digital era, has now become regulated by DRM in the digital era. Lessig believes that fair use, which was traditionally used as a defense for content regulated by copyright law, now also carries the burden of being a defense for DRM regulated content,[40] and that free dissemination of content and derivative creativity may be further encumbered.

Critics believe that a proprietary model comprised of a full implementation of DRM and trusted systems could result in the suppression of creativity.[41] Yochai Benkler describes this lockdown as a part of a larger battle between the market-based, proprietary models that serve mass media and "pharmaceutical-style" innovation, and the commons-based and nonproprietary model of production.[42] Jonathan Zittrain refers to the transformation of all-purpose technologies to "tethered appliances."[43] Specifically, the personal computer may be converted from a substantially programmable and customizable machine into a tethered appliance like a telephone, which is constructed for very specific functionality as designed by its proprietor. As such, the DRM lockdown can turn general-purpose, smart computers into special-purpose, dumb computers, thereby undermining the democratic and innovative potential of networks, the

---

[38] *See* LAWRENCE LESSIG, FREE CULTURE 131-182 (2004). *See also* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (2000) (suggesting that DRM-like computer code can regulate conduct much like legal code); LAWRENCE LESSIG, CODE: VERSION 2.0 (2006) (updating the argument that computer code can regulate conduct); James Grimmelmann, *Regulation by Software*, 114 YALE L.J. 1719 (2005) (elaborating on Lessig's proposition that "code is law.").

[39] Noguchi, *supra* note 24, at 7-8.

[40] FREE CULTURE, *supra* note 38, at 143-45.

[41] *See* BENCKLER, *supra* note 10; Gillespie, *supra* note 2, at part 3, ch. 11; FREE CULTURE, *supra* note 38.

[42] *See* BENCKLER, *supra* note 10, at 381.

[43] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 3 (2008).

Internet, and media.[44] The Internet in particular could undergo a transformation from what Jonathan Zittrain has called a generative network to an appliance-based network due to DRM, trusted systems, and Web 2.0 applications. Such a transition, these critics argue, is dangerous and would destroy the creative potential of the Internet.[45]

Benckler also suggests that lobbyists advocating expanded content regulation via copyright and DRM are merely engaged in rent-seeking.[46] This line of argument suggests that Congress has a responsibility to preserve content for the public good as opposed to merely serving corporate lobbies, and that the over-expansion in general of intellectual property rights burdens creativity rather than incentivizing it.[47] Tarleton Gillespie and Dan Burk further argue that DRM and trusted systems represent an overly paternalistic view of information users as entities who are incapable of making decisions themselves.[48]

Moreover, critics note that absent regulation, most trusted systems have not been successful either because they are easily hacked into or because they have not proven marketable.[49] Going further, even if trusted systems were impenetrable and could not be subverted, recording analog copies of content remains simple.[50] For example, a user can record content by placing a microphone next to a DRM-

---

[44] *Id.* at 8.

[45] Generative networks allow users to customize their networks to meet their needs, whereas an appliance-based network is restricted to pre-defined uses set by a proprietor. *See* ZITTRAIN, *supra* note 43; FREE CULTURE, *supra* note 38; BENCKLER, *supra* note 10.

[46] BENCKLER, *supra* note 10, at 461.

[47] *See* Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354 (1999); Yochai Benkler, *Through the Looking Glass: Alice and the Constitutional Foundations of the Public Domain*, 66 LAW & CONTEMP. PROBS. 173, 216–18 (2003); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999); Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 50–51 (2001).

[48] Dan Burk & Tarleton Gillespie, *Autonomy and Morality in DRM and Anti-Circumvention Law*, 4 TRIPLE C 239 (2006).

[49] ZITTRAIN, *supra* note 43, at 105; Joan Feigenbaum & Peter Swire, *Control of Personal Information: A Dialogue Between a Technologist and a Lawyer*, Slide 17, Radcliffe Inst. and Harvard Div. of E&AS Symposium on Security and Privacy (2004).

[50] ZITTRAIN, *supra* note 43, at 115.

protected audio player. Finally, as long as the all-purpose PC remains a central component of networks and the information stream, the ability to implement trusted systems will remain limited.[51] This is because users will still utilize their PCs in a generative fashion, and trusted system restrictions will not substantially limit users' abilities to customize their PCs to perform any desired tasks.[52]

The DMCA has also fallen under intense criticism. Critics assert that the bundle of rights granted by a copyright is not exclusive in the sense that real property rights are exclusive. Thus, there are many uses of copyrightable materials—such as fair uses and even uses of public domain works—that courts have always held to be non-infringing, yet these uses are nevertheless criminalized by the DMCA. For example, the DMCA criminalizes circumventing DRM restrictions in e-book readers even for novels in the public domain.[53]

Further, some critics have argued that the DMCA is both vague and overbroad, resulting in civil and/or criminal liability for parties who many argue should be exempt from anti-circumvention liability. For example, while the DMCA includes an exemption for researchers,[54] the overall provision is vague and has thus adversely affected the cryptography research community.[55] In one case, when Edward Felten, a computer science professor at Princeton University, planned to present a paper on weaknesses of certain encryption technologies at an academic conference, several proprietors subsequently threatened him with a DMCA lawsuit.[56] Thus, the DMCA has gone so far as to curtail academic freedoms.

Skeptics even wonder whether the DMCA accomplishes what it set out to do: namely, to prevent piracy. Even if the DMCA successfully deters the circulation of anti-circumvention software, which is debatable, the existence of similar unprotected content elsewhere may

---

[51] *Id.* at 123.

[52] *Id.* Also, the ability for networks to block streams of incoming information or regulate the speed with which the network can access the streams can further segregate networks and transform them into appliances. BENCKLER, *supra* note 10, at 397-98. This has given rise to the network neutrality movement, which criticizes these information exchange gradients.

[53] BENCKLER, *supra* note 10, at 415.

[54] 17 U.S.C. § 1201(g) (2000).

[55] BENCKLER, *supra* note 10, at 416.

[56] FREE CULTURE, *supra* note 38, at 155-57.

draw consumers to those sources. It takes only a single person to decrypt content and upload it to the Internet.[57] In order to be worthwhile, anti-circumvention laws need to be part of a comprehensive approach in regulating *all* sources of content, an increasingly difficult task in the digital information age.

Critics also allege that ever-expanding copyright laws over-protect content, which is a concern because DRM coupled with strong copyright laws creates a restrictive climate for consumers.[58] Intense lobbying by mass-media industries has resulted in copyright term extensions that continue to prevent copyrighted materials from falling into the public domain.[59] Moreover, the scope of copyrightable materials has slowly expanded to cover virtually all forms of creativity, including performances and broadcasts. Copyrights are generally available without registration and inhere in a creative work,[60] thus providing for protection that content-owners might otherwise forego if registration were required.

IV. HOW TRUSTED SYSTEMS CAN PROTECT PERSONAL INFORMATION

Technological measures conferring protection to creative content can be similarly used to safeguard sensitive personal information, although these measures must be specifically tailored to that end. In this regard, trusted systems have great potential. Trusted systems require devices to enforce rules defined by proprietors.[61] Such rules may be built into devices, embedded in content, or sent by licensing authorities when users initiate functions requiring authorization.[62] For example, trusted systems may only allow users to access protected content if the users' personal computers ("PCs") provide identification

---

[57] Timothy B. Lee, *Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act*, CATO INSTITUTE POLICY ANALYSIS no. 564, Mar. 21, 2006, at 12, *available at* http://www.cato.org/pub_display.php?pub_id=6025.

[58] BENCKLER, *supra* note 10, at 395.

[59] The most recent term extension was in 1998, which extended copyrights for an additional twenty years. *See* Copyright Term Extension Act, Pub. L. No. 105-298, 11 Stat. 2827 (1998).

[60] 17 U.S.C. § 408(a) (2000) (stating that "registration is not a condition of copyright protection.").

[61] GILLESPIE, *supra* note 2, at 52.

[62] *Id.*

data in order to authorize access. Another example is trusted printing, where an online work will only print if payment is first made, the work is sent to the printer in encrypted form, and the copies are watermarked.[63]

Proponents of trusted systems argue that their utility in protecting personal information is especially high in light of our lack of ability to prevent misuse of information by parties who have access to it. Thus, the only remaining way to control this misuse is to block anyone's ability to access that information; trusted systems are one way to do that.[64] However, since there is no absolute method to prove trust, trusted systems are typically incapable of flagging all untrustworthy access attempts.[65] Therefore, a layered approach that authenticates access through a variety of means would be most effective.[66] A comprehensive and working approach should be comprised of a combination of hardware, software, people, procedures, and law.[67] Technological protection, including hardware and software-based methods, is necessary but not sufficient to secure data; therefore, the law needs to work in tandem with technology to better ensure that these systems properly protect information privacy.[68]

Software-based management rights, such as data masking,[69] role based access controls,[70] VIP systems,[71] or logging and audits,[72] are useful in preventing routine violations by employees who attempt to

---

[63] Greenleaf, *supra* note 1, at 44.

[64] Feigenbaum & Swire, *supra* note 49, at Slide 8.

[65] Taipale, *supra* note 5, at 167.

[66] *Id.*

[67] Feigenbaum & Swire, *supra* note 49, at Slide 30, 34-35.

[68] *Id.* at Slide 21-22.

[69] Data masking provides a layer of protection by in this context de-identifying personal data. Peter Swire, *Peeping*, BERKELEY TECH. L.J. (forthcoming) at *23-25, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1418091.

[70] Role based access controls only allow people in authorized roles to perform given activities in a computer system. *Id.* at 19-20.

[71] VIP systems can provide extra procedures for persons who are likelier targets. *Id.* at 20-22.

[72] A computer system can log access attempts and audit the logs in order to "deter, detect, and prove privacy violations." *Id.* at 25-27.

"peep" into restricted work databases. However, software-based measures have limited enforceability in that they may still be susceptible to advanced and determined cryptographic attacks.[73]

Hardware can supplement software to provide a stronger approach. Trusted systems that utilize "hardware-based, cryptographic support" can be implemented to prove that a machine accessing the data is running a particular software stack.[74] However, there are numerous hurdles before such a method can be implemented. These systems require a high level of technical sophistication to build, to say nothing of the business and legal concerns mentioned earlier.[75] Further, these systems are still subject to information leakage, which is arguably a greater threat than circumvention.[76]

Prevention of peeping is also bolstered through procedure. For example, employee training and sanctions may deter employees from engaging in unauthorized information gathering.[77] Requiring notice to individuals following an unauthorized access may also help prevent security breaches.[78]

Legal protections constitute a final layer. As discussed earlier, the DMCA makes circumvention of trusted systems unlawful.[79] Additionally, U.S. information privacy law safeguards the privacy of certain sensitive records.[80]

---

[73] Feigenbaum & Swire, *supra* note 49, at Slide 18.

[74] *Id.*

[75] *Id.*

[76] *Id.* at slide 19.

[77] Swire, *supra* note 69, at 27-28.

[78] *Id.* at 28-31. California has passed the first piece of legislation mandating these notices.

[79] *See* Digital Millennium Copyright Act, *supra* note 13.

[80] For example, the Health Insurance Portability and Accountability Act, governs when medical records can be disclosed. *See* Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936.

V. HOW DRM AND TRUSTED SYSTEMS CAN INFRINGE CONSUMER PRIVACY

The ability of DRM and trusted systems to protect content or data is complicated by concurrently-arising privacy concerns. Proprietors can collect personal information of users who perform transactions with respect to this data or content via DRM-enabled devices.

Defining privacy is a prerequisite to fully exploring DRM's privacy-invasive implications. Most definitions incorporate at least one of two main components. First, intellectual privacy includes personal autonomy that guarantees "breathing space for thought, exploration, and personal growth."[81] Second, intellectual privacy concerns spatial privacy that allows for intellectual consumption beyond public view.[82]

In view of these definitions, DRM and trusted systems may usher in a host of privacy concerns, shifting the balance in favor of content owners over content users.[83] DRM may infringe upon the privacy of consumers both under the personal autonomy definition as well as the spatial privacy definition.[84] First, DRM's ability to constrain intellectual choice implicates the personal autonomy definition.[85] Second, its monitoring capability intrudes upon spatial privacy.[86] Third, DRM's "self-help" function may give rise to privacy violations under both the personal autonomy and spatial privacy definitions.[87]

---

[81] Cohen, *supra* note 6, at 577-78.

[82] *Id.* at 578-579.

[83] Greenleaf, *supra* note 1.

[84] Cohen, *supra* note 6, at 580.

[85] *Id.* at 580-584. However, this argument is somewhat undercut by the fact that many products already deprive intellectual choice. For example, access to a limited number of television channels could be perceived as a limitation on intellectual choice. Many further argue that loss of intellectual choice is actually a loss of liberty, not privacy.

[86] *Id.* at 580-86.

[87] *Id.* at 586-88. Self-help features in DRM refer to automated mechanisms that could regulate access if a user attempts an unauthorized use. This feature could be implemented through external control by communicating user activity to a host. On the other hand, this functionality could be controlled through internal pre-defined DRM logic, with no communication to outside entities.

Of these three functions, DRM's monitoring capability has garnered the majority of attention.[88] While some DRM does not report a user's activities back to the technology's proprietors, other types of DRM lockdowns *do* report information back, infringing upon the user's privacy.[89] Such strict DRM creates several privacy concerns for content users. The users can be identified and owners can collect their data on a mass scale, especially when users access content by submitting unique identifiers.[90] What's more, some trusted systems distribute user data without a user's knowledge and may build user profiles.[91] Personalized marketing schemes based on these user profiles may deprive users of individual choice and intellectual freedom.[92] Thus, the trusted systems' "[m]onitoring of reading and viewing habits poses the threat of a *'chilling effect' on freedom to read, think, and speak.*"[93] Further, consumers could be disincentivized from conducting fair uses that inconveniently require permission.[94]

For time immemorial, the unregulated private sphere has been a place where individuals can conduct anonymous transactions in the privacy of their homes. However, this private sphere risks being obviated by a world in which proprietors observe and record all user activities.

How copyright monopolists threaten this private sphere via DRM is well-documented. In the pre-DRM world, many sales of artifacts containing content (*e.g.* books) were anonymous, and consumers rarely entered into contracts directly with content providers, and

---

[88] *Id.* at 577-78.

[89] *Id.* at 585-86.

[90] Jonathan Weinberg, *Hardware-Based ID, Rights Management, and Trusted Systems*, 52 STAN. L. REV. 1251 (2000); Cohen, *supra* note 6, at 575-76.

[91] *See* Weinberg, *supra* note 90.

[92] *See* Paul Ganley, *Access to the Individual: Digital Rights Management Systems and the Intersection of Informational and Decisional Privacy Interests*, 10 INT'L J.L. & INFO. TECH. 241, 241 (2002).

[93] Greenleaf, *supra* note 1, at 49.

[94] Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49 (2006).

instead dealt with intermediaries (*e.g.* bookstores).[95] Such artifacts never had any built-in surveillance technologies.[96] Owners could not control artifacts containing the content and did not know if users loaned artifacts to one another.[97] Copyright enforcement was selective and periodic rather than an all-encompassing real-time surveillance of infringement, and various fair uses of artifacts were available.[98] In sum, many types of infringement could only be caught in public, effectively creating a private sphere unregulated by copyright law.[99] Critics believe that the existence of this private sphere is one way to accommodate public welfare in response to an otherwise extreme copyright monopoly.[100] They contend that an implementation of DRM and/or expanded copyright regimes would disturb this proper balance, tipping regulation in favor of copyright owners and severely curtailing the privacy rights of consumers.[101]

Many DRM proponents accept that DRM significantly expands the scope of protection, and argue instead that the copyright system was always intended to give a maximal level of protection to content owners.[102] They do not accept the notion that pre-DRM limitations properly served the public welfare by balancing against a more comprehensive copyright monopoly.[103] These proponents believe that regulating the private sphere is appropriate and finally feasible in view of DRM technologies that lower the transaction costs of protecting copyright compared to the pre-DRM world.[104]

---

[95] Greenleaf, *supra* note 1, at 37. Of course, credit card sales have long posed information privacy concerns even before the existence of DRM.

[96] *Id.* at 37.

[97] *Id.* at 37-38.

[98] *Id.* at 38.

[99] *Id.*

[100] Greenleaf, *supra* note 1, at 39.

[101] The implementation of various business models may also have an impact, for example the motivations of third-party intermediaries as far as whether they are neutral parties may depend on the business models in which they operate. *Id.* at 51.

[102] *Id.* at 39.

[103] *Id.*

[104] *Id.*

A distinct privacy concern arises due to the potential for "collateral damage" from criminalizing a large percentage of the population who have committed copyright violations.[105] The risk in such mass criminalization is that it becomes "trivial, as a matter of due process, to effectively erase much of the privacy most would presume" for law-abiding citizens as compared to criminals.[106] This deprivation of privacy could include the loss of information privacy. For example, copyright infringers may no longer be secure against authorities who may seize infringers' computers and deny them access to the Internet.[107] The DRM lockdown exacerbates the problem through the creation of ever more copyright criminals.

Privacy risks to the private sphere remain equally salient with respect to trusted systems designed to protect data. In trusted systems, the multi-layered authentication process leaves proprietors ample opportunity to collect user ID data. If all devices, such as PCs, bought by consumers for the home or implemented by companies utilize trusted systems, the public at large would find it difficult to escape their watchful eye when performing any kind of digital transaction. This statement continues to be true regardless of whether the transaction is for obtaining copyrighted content or utilizing a computer system for any other purpose.

The DMCA attempts to address the foregoing concerns by including an exemption for individual end users to circumvent access controls if their purpose is to destroy ID data.[108] However, two problems arise. First, this exemption has limited scope, and second, if circumvented files are altered, they may be rendered "untrusted" and therefore unusable.[109] Another DMCA provision preserves all federal and state privacy protections relating to Internet usage.[110]

---

[105] FREE CULTURE, *supra* note 38, at 205.

[106] *Id.*

[107] *Id.* (quoting Fred von Lohmann).

[108] 17 U.S.C. §1201(i) (2000).

[109] Ryan Roemer, *Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, 2003 UCLA J.L. & TECH. 8, part V(A)(4)(b) (2003).

[110] 17 U.S.C. §1205 (2000).

VI. NEGOTIATING A BALANCE OF RIGHTS BETWEEN PROPRIETORS AND USERS

Scholars have suggested several ways of implementing DRM and trusted systems in order to preserve the data rights of proprietors while also demarcating the proper boundaries of the private sphere by safeguarding users' privacy, access, and fair use rights. For example, Weinberg, Cohen, and Woodford have recommended solutions applicable to all types of DRM. Noguchi, Burk, Cohen, Mulligan and Burstein have proposed DRM designs effective for copyright-specific purposes, although these designs can be similarly applied to trusted systems that protect data. Many of these systems can be implemented in combination as well.

A. SOLUTIONS THAT ARE EXPLICITLY APPLICABLE TO ALL DRM IMPLEMENTATIONS

Weinberg notes that trusted systems incorporating unique identifiers traceable to users provide maximal benefit to owners at the expense of user privacy, and therefore suggests balancing the equation by allowing users to access content with pseudonymous identifiers.[111] This is feasible because supplying login credentials does not inherently require providing identity. The above approach largely preserves content owners' rights, although it prevents owners from discriminating among users based on a particular characteristic unless users provide information relating to that characteristic.[112] As this method posits an authentication process that is public and open to scrutiny, content owners would be deterred from performing unpopular actions,[113] which would be a socially desirable outcome.

Cohen advocates a value-sensitive framework for DRM design.[114] With regard to privacy, Cohen suggests that DRM be designed to: (1)

---

[111] Weinberg, *supra* note 90, at 1279-80. A pseudonymous identifier is an encrypted name that is associated with the user in particular contexts, but does not allow a content owner to probe associations with a user's names in other contexts. *Id.* at 1279. For an alternative version implementing pseudonymous credentials, *see* Claudine Conrado et al., *Privacy-Preserving Digital Rights Management*, Secure Data Management: VLDB 2004 Workshop, SDM 2004, LNCS 3178, at 83 (Willem Jonker & Milan Petkovié eds., 2004).

[112] Weinberg, *supra* note 90, at 1280.

[113] *Id.* An unpopular action could for example be a content owner's distribution of collected user information without user permission.

[114] Cohen, *supra* note 6, at 609-16.

minimize direct constraints on intellectual choice in the private sphere, (2) limit collection of user information to instances where the information is necessary for a significant aim, and (3) limit DRM devices' "self-help" functionality.[115] If non-privacy related benefits, such as a content owner's rights, are affected, then a choice needs to be made that explicitly outlines which values are being favored.[116] Cohen also proposes expanding the role of privacy tort law and consumer protection law to protect users.[117]

Woodford suggests granting the FCC statutory authority to regulate DRM, given the FCC's requisite technical expertise and historical experience in safeguarding the public interest.[118] The FCC could ensure personal privacy by requiring encryption of private information when it is used for authentication, and by articulating explicit policies regarding private information.[119] The FCC can tailor these protections to different DRM technologies through case-by-case oversight.[120] The FCC could also regulate DRM systems to be designed in "modular" ways to accommodate evolving fair use standards in an efficient manner.[121] A modular design would allow specific code segments that define fair uses to be swapped easily, enabling DRM systems to continually update as fair use laws change.[122]

B. NOMINALLY COPYRIGHT-SPECIFIC DESIGNS

Various proposed systems specifically tailored for copyright offer promise in striking a balance between copyright owners and users. Some early examples include fair use determinations by owners, purely automatic software algorithms, or escrow agents. An escrow

---

[115] *Id.* at 611-13.

[116] *Id.* at 612.

[117] *Id.* at 589-609.

[118] Chad Woodford, *Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management*, 75 U. COLO. L. REV. 253, 291-92 (2004).

[119] *Id.* at 294.

[120] *Id.*

[121] *Id.* at 293.

[122] *Id.*

agent is a trusted third-party decision-maker such as a public regulatory body.[123] Critics have objected to owners making such determinations on grounds that owners might improperly apply fair use law, intrude upon user privacy and anonymity, and chill spontaneous uses due to a lengthy and complicated approval process.[124] The algorithm version provides privacy and efficiency benefits, but there is a lingering concern that purely algorithm based DRM technologies cannot make effective, case-by-case judgment calls as to which content to exclude from DRM protection in the same way that human decision-makers can.[125] U.S. fair use law is vaguely defined, creating challenges in implementing a workable algorithm that correctly determines when a use is a fair use.[126] On the other hand, escrow agents can effectively determine fair uses, and if user ID records are subject to stringent protections, they can also preserve user privacy.[127] Still, requiring permission from escrow agents for all fair uses may be inefficient.[128]

Burk and Cohen have suggested a hybrid two-layer DRM mechanism comprised of an automatic algorithm and an escrow agent.[129] The first layer of this mixed fair use infrastructure constitutes a set of automatic fair use defaults based on "customary norms of personal noncommercial use," and thereby provides swift authorization for clear fair uses.[130] For uses not covered by the first

---

[123] Burk & Cohen, *supra* note 47, at 63.

[124] *Id.* at 59-60.

[125] Noguchi, *supra* note 24, at 9.

[126] Armstrong, *supra* note 94, at 84. Since European copyright law's exemptions are more discrete, automatic fair use algorithms are more effective, although they still cannot match human decision-makers. Burk & Cohen, *supra* note 47, at 70.

[127] Burk & Cohen, *supra* note 47, at 63-64.

[128] *Id.* at 64.

[129] Armstrong, *supra* note 94, at 82-83; Burk & Cohen, *supra* note 47, at 65-66. Burk and Cohen have also recently classified five theoretical models for understanding consumer interests, and have suggested how to proceed based on those frameworks. *See* Dan Burk & Julie Cohen, *Models of Consumer Protection in DRM*, Copyright, Digital Rights Management Technology and Consumer Protection Symposium, University of California-Berkeley Boalt Hall School of Law, *available at* http://www.law.berkeley.edu/institutes/bclt/copyright/presentations/Cohen.pdf (March 9, 2007).

[130] Burk & Cohen, *supra* note 47, at 65.

layer, the second layer would allow users to seek access permission from the escrow agent, and the escrow agent would send back digital keys if the use is authorized.[131] This hybrid system would offer robust fair use protection due to the automatic layer, efficient protection via a comprehensive two-tiered approval system, and correct application of fair use law through nonbiased algorithms and third-parties. This design also protects user privacy rights by eliminating the need for content owners to directly monitor and approve fair uses and by requiring escrow agents to implement strict privacy-protective procedures. However, uses that straddle the boundary of what constitutes a fair use are precisely those uses that invoke the most substantial privacy concerns, given that they may be infringing. Since escrow agents may collect ID data, they may not be able to provide fully anonymous pre-DRM-type fair uses.[132]

Armstrong has set forth a modified version of this mixed fair use infrastructure. In his model, if the automatic algorithm denies access, a user has the option of petitioning the escrow agent for access, or forcing access through a *quid pro quo* arrangement if the user deems the escrow agent method to be burdensome.[133] This *quid pro quo* arrangement would mandate users to provide contextual information for recording in an audit trail in exchange for access.[134] This audit trail could be implemented via pseudonymous credentials in order to preserve user privacy, and owners could only access and be allowed to decrypt these credentials if they believe a user is committing substantial infringement.[135] Armstrong suggests that this audit trail ensures that a user's ability to force access does not entirely declaw DRM systems.[136]

Mulligan and Burstein have proposed another model that could preserve privacy for users conducting fair uses.[137] They suggested

---

[131] *Id.* at 65-66. Burk and Cohen suggest the Library of Congress as an example of a public organization that could inhabit this role, but are skeptical over whether a private organization could do so. *Id.* at 66-67.

[132] Armstrong, *supra* note 94, at 88.

[133] *Id.* at 100-01.

[134] *Id.* at 101.

[135] *Id.* at 106-07.

[136] *Id.* at 102.

[137] *Id.* at 91 (citing Deirdre Mulligan & Aaron Burstein, *Implementing Copyright Limitations in Rights Expression Languages*, Digital Rights Management: ACM CCS-9

improving fair use protections by altering current Rights Expression Languages ("RELs"),[138] including XrML,[139] to make the expression of context-dependent policies, like fair use, easier.[140] They also recommend adding a new messaging protocol to XrML that lets end users assert rights over content in their possession.[141] Their system would restore certain fair use rights by allowing numerous default positions for different media types, rather than a one-size-fits-all approach that is not sensitive enough to recognize context-dependent policies.[142] They would also implement protective measures to ensure that their system would not become a tool for surveillance by copyright owners.[143] For example, the DRM system would not record a user's personally identifying information or usage statistics, ensuring that copyright owners could not use that information to bargain with users for rights that are freely available under the fair use doctrine.[144] Fox and LaMacchia have set forth a similar system of negotiated safe-harbors expressed in RELs for clear fair uses.[145]

Another approach involves a programming language called LicenseScript that is used specifically in DRM in order to overcome problems with XML based languages.[146] It can be cumbersome to program complex conditional rules in XML-based RELs and even

---

Workship, DRM 2002, LNCS 2696, at 137, 139 (Joan Feigenbaum ed., 2003), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/copyright_rights_expression.pdf).

[138] A Rights Expression Language ("REL") defines user rights with respect to files and processes on a machine. For example, such a language can control file access, printing, or copying to a clipboard.

[139] XrML (eXtensible Rights Markup Language) is an REL that is utilized for the MPEG-21 multimedia format.

[140] Armstrong, *supra* note 94, at 91.

[141] *Id.*

[142] *Id.* at 93.

[143] *Id.*

[144] *Id.* at 94.

[145] Barbara L. Fox & Brian A. LaMacchia, *Encouraging Recognition of Fair Uses in DRM Systems*, Commc'ns of the ACM, Apr. 2003, at 61.

[146] *See* Cheun Ngen Chong et al., *LicenseScript: A Novel Digital Rights Language and its Semantics*, http://purl.org/utwente/fid/1152 (2003); Armstrong, *supra* note 94, at 94-96.

impossible to express many context-specific rules requiring data input that lie at the heart of many copyright exemptions.[147] LicenseScript purports to solve these issues. This approach is far more deferential to copyright holders and records all instances of fair use.[148] Still, some have noted that this basic technological model could be modified to more properly protect fair use.[149]

Noguchi has offered several broad recommendations on DRM configuration that will: (1) allow the creation and use of private copies, (2) allow content to be given to family and friends, (3) allow users to preview content, and (4) exclude the public domain from DRM protection.[150]

Broadly speaking, the core aim of these copyright-based designs are to define accesses and uses that are allowed versus those that are forbidden, to ensure that these designs do not entail collection and abuse of users' private information, and to provide quick and ideally instantaneous access upon user request. This general framework is applicable to any situation governing user access and data use in a computer system, including the scenario of users accessing trusted systems that protect personal information. Specifically, a mixed-use architecture with a layered design and context-specific definitions in RELs can be used for corporate information access rules in addition to fair use rules.

C. COMBINING THESE APPROACHES AND LOOKING AHEAD

Many of these proposals are not mutually exclusive and can thus be simultaneously implemented in one, multi-tiered approach. The following discussion describes how the foregoing solutions can be implemented together. Users could access trusted systems using pseudonymous identifiers through a layered authentication process which uses RELs to define context-specific access and use rules in the first layer, and a user option of an escrow agent or forced access in the second layer. The escrow agent should erase user-specific records of access to maintain user trust in making second-layer requests and to protect user privacy. At most, the escrow agent should collect only

---

[147] *Id.* at 94-95.

[148] *Id.*

[149] *Id.* at 99.

[150] Noguchi, *supra* note 24, at 8.

anonymous use data if for example this data could help streamline the escrow agency system. The forced access option should require owners to access the audit trail to reveal potentially infringing uses only under exceptional circumstances. Finally, the REL codes could be programmed in a modular fashion so that these context-specific rules could be altered quickly.

Public regulatory oversight is a promising option to ensure that DRM architectures do not lag behind quickly evolving fair use laws or information access standards. Further, a one-size fits all approach is dangerous given the myriad uses of DRM and trusted systems for protecting varying types of information. The FCC would be a logical candidate for the regulatory oversight role and could provide a repository of modular REL codes that are updated according to new laws and standards for different DRM devices and applications. Although this entails the intervention of a public regulatory body for REL code updates as well as another regulatory body like the Library of Congress to serve as an escrow agent, this approach still prevents bureaucratic inefficiencies from chilling spontaneous uses, due to the existence of the forced access option. Moreover, the existence of the forced access option ensures that users do not inundate escrow agents with requests, thus avoiding the creation of a bloated regulatory body and large request backlogs.

This implementation is clearly deferent to users compared to owners, given that users have near carte blanche access privileges that cannot be monitored by owners unless the audit trails evince flagrant misuses of user privilege. However, the protection conferred upon owners still exceeds the pre-DRM world, and a precipitous change to a universal owner-centric DRM lockdown would disrupt the social and creative dynamic, as this paper has emphasized.

Still, owners can rest assured that as artificial intelligence evolves to better define context-dependent policies, the need for the second layer of the mixed-use architecture will be gradually swallowed by the artificial intelligence of the first layer. A fully developed artificial intelligence will eventually provide virtually all the necessary access rights and privacy protections to users, while limiting the ability of users to circumvent DRM restrictions on legitimately protected data.

VI. CONCLUSION

DRM is here to stay, so the lingering issue is its ultimate role. Legal, policy, social and technological changes are all relevant to DRM, yet these changes are rarely considered together. A comprehensive approach involving changes in all of these areas is

necessary to set forth a rational implementation of DRM that accommodates proprietors' rights in content or data, and preserves users' privacy, access, and fair use rights.